TECNOLOGÍA QUE CONECTA

PLANTILLA PRÁCTICA · 2026

Plan de respuesta a incidentes: los primeros 60 minutos

Qué hacer, quién decide y a quién llamar cuando ocurre un incidente de ciberseguridad. Imprímelo, complétalo con tu equipo y tenlo a mano antes de necesitarlo.

En esta plantilla

1. **Los primeros 60 minutos**
   Cuatro etapas, paso a paso.
2. **Quién hace qué**
   Los roles clave durante un incidente.
3. **Decisiones rápidas**
   Qué hacer según lo que está pasando.
4. **Hoja de contactos**
   Para completar e imprimir.

PARTE 1

Los primeros 60 minutos

Las primeras decisiones definen cuánto daño causa un incidente. Sigue estas etapas en orden y anota la hora de cada acción.

0–15 MIN
ETAPA 1

Detecta y confirma

- Confirma que es un incidente real y anota la hora en que se detectó.
- **No apagues** los equipos afectados: se pierde evidencia.
- Avisa de inmediato al líder de incidente definido en este plan.

15–30 MIN
ETAPA 2

Aísla

- Desconecta de la red los equipos afectados (cable y Wi-Fi).
- Bloquea o cambia las contraseñas de las cuentas comprometidas, desde un equipo limpio.
- Conserva la evidencia: no borres correos, archivos ni registros.

30–45 MIN
ETAPA 3

Evalúa y escala

- Define el alcance: qué sistemas, datos y áreas están afectados.
- Clasifica la gravedad: crítica, alta o media.
- Activa el apoyo externo: tu proveedor de seguridad, tu aseguradora y tu asesor legal.

45–60 MIN
ETAPA 4

Comunica y documenta

- Informa a la dirección con hechos, no con suposiciones.
- Define un mensaje único para el personal y, si hace falta, para clientes.
- Si hay datos personales involucrados, evalúa con tu asesor legal las obligaciones de notificación.

LO QUE NUNCA DEBES HACER

No apagues los equipos · No borres evidencia · No pagues un rescate sin asesoría legal y especializada · No coordines la respuesta por el correo comprometido.

PARTE 2

Quién hace qué

Define estos roles antes de que ocurra un incidente. En empresas pequeñas, una persona puede cubrir más de un rol.

Líder de incidente

Coordina la respuesta, toma las decisiones operativas y lleva el registro de lo que se hace.

Responsable técnico

Aísla equipos, revisa registros y trabaja con el proveedor de seguridad.

Dirección

Aprueba decisiones de alto impacto: detener operaciones, comunicar a clientes o contratar apoyo.

Legal y cumplimiento

Evalúa obligaciones legales, contratos, seguros y notificaciones.

Comunicación

Prepara los mensajes para el personal, los clientes y, si hace falta, los medios.

PARTE 3

Decisiones rápidas

¿Hay archivos cifrándose o una nota de rescate?	→ Aísla de inmediato los equipos afectados y protege los respaldos desconectándolos de la red.
¿Hay datos personales de clientes o empleados involucrados?	→ Involucra a legal desde el primer momento para evaluar obligaciones de notificación.
¿Se detuvo una operación crítica del negocio?	→ Escala a la dirección y activa los procedimientos alternos de operación.
¿Te piden un pago para recuperar la información?	→ No pagues ni respondas sin asesoría legal y especializada. Pagar no garantiza recuperar los datos.
¿El correo corporativo está comprometido?	→ Coordina por un canal alterno definido de antemano (teléfono o mensajería).

PARTE 4

Hoja de contactos

Complétala, imprímela y guarda una copia fuera de los sistemas de la empresa: durante un incidente, el correo y la red pueden no estar disponibles.

Rol	Nombre	Teléfono	Alterno
Líder de incidente			
Responsable de TI			
Proveedor de seguridad / SOC			
Proveedor de internet			
Dirección general			
Asesor legal			
Aseguradora de ciberriesgo			
Comunicación / Recursos Humanos			
Fabricantes o proveedores críticos			

Información que debes tener a mano

- [ ] Dónde están los respaldos y cómo se restauran.
- [ ] Credenciales de emergencia guardadas fuera de línea, en un lugar seguro.
- [ ] Lista de sistemas críticos y su orden de recuperación.
- [ ] Número de póliza de ciberriesgo, si la tienes.

VIVA SOLUTIONS · NOC Y SOC 24/7 DESDE PANAMÁ

¿Quieres un plan a la medida de tu empresa?

Te ayudamos a definir roles, procedimientos y contactos, y a ponerlos a prueba con un simulacro, para que tu equipo sepa exactamente qué hacer cuando ocurra un incidente.

Habla con un ingeniero: vivaconecta.com/#contacto
(507) 216-9004 · webforms@vivaconecta.com

viva
TECNOLOGÍA QUE CONECTA

Plantilla orientativa de buenas prácticas. No sustituye la asesoría legal ni un plan formal adaptado a tu organización.